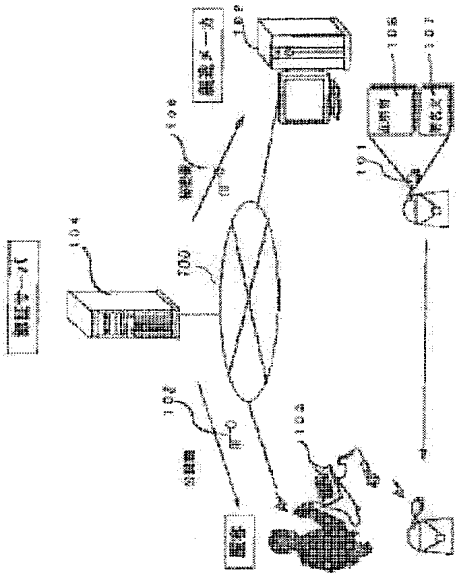
X1

PRODUCT AUTHENTICATION SYSTEM AND MERCHANDISE TAG TO BE USED FOR THE SAME SYSTEM

Publication number: JP2000011114 (A)
Publication date: 2000-01-14
Inventor(s): KIKUCHI YOSHITOMO; TSUCHIDA TOSHIKATSU +
Applicant(s): HITACHI LTD +
Classification:
- international: ***G06K17/00; G06K19/07; G06Q10/00; G06Q30/00; G06Q50/00; G09C1/00; H04L9/32;*** **G06K17/00; G06K19/07; G06Q10/00; G06Q30/00; G06Q50/00; G09C1/00; H04L9/32;** (IPC1-7): G06F17/60; G06K17/00; G06K19/07; G09C1/00; H04L9/32
- European:
Application number: JP19980175500 19980623
Priority number(s): JP19980175500 19980623

Abstract of **JP 2000011114 (A)**

PROBLEM TO BE SOLVED: To provide a system for confirming whether or not a product is real or a fake by allowing a manufacture maker to record certificate data in the memory of a merchandise tag while adding an electric signature to the certificate data, and to ship the product after attaching this tag to this product, and allowing a purchaser to read this certificate data by an exclusive reader in a shop. SOLUTION: At the time of shipping a product, a merchandise tag 101 in which certificate data for certifying the manufacture of the product by the maker are recorded is issued by a merchandise tag issuing machine 102, and this product is shipped after attaching the merchandise tag to the product. A purchaser in a shop reads and confirms the certificate from the merchandise tag 101 by a merchandise tag reading terminal 103. The purchaser of the product previously inputs the certificate decoding information from a certification server 104 through a network and mailing or the like to the reading terminal 103, and collates the certificate information of the merchandise tag 101 in the shop for confirming whether the product is real or a fake.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－11114
（P2000－11114A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｃ０６Ｋ　17/00	Ｔ	５Ｂ０３５
Ｇ０６Ｆ　17/60		Ｃ０９Ｃ　1/00	６４０Ｂ	５Ｂ０４９
Ｇ０６Ｋ　19/07		Ｃ０６Ｆ　15/21	Ｚ	５Ｂ０５８
Ｇ０９Ｃ　1/00	６４０	Ｃ０６Ｋ　19/00	Ｈ	５Ｋ０１３
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｄ	

審査請求　未請求　請求項の数４　ＯＬ　（全６頁）

(21)出願番号　特願平10－175500

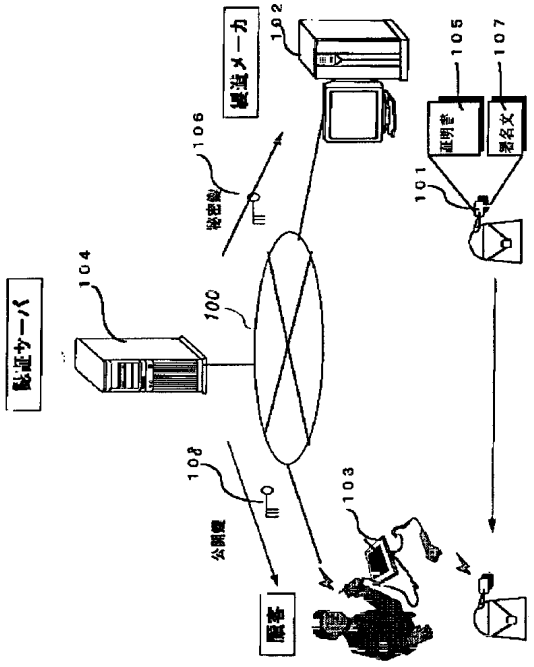
(22)出願日　平成10年６月23日(1998.6.23)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　菊地　良知
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所システム開発本部内
(72)発明者　土田　稔勝
神奈川県横浜市戸塚区戸塚町216番地　株式会社日立製作所情報通信事業部内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

最終頁に続く

(54)【発明の名称】　製品認証システムおよびそれに用いる商品タグ

(57)【要約】
【課題】　商品タグに製造メーカが証明書データに電子署名を付けて商品タグのメモリ内に記録し、これを製品につけて出荷、購入者が店舗にて専用のリーダでこれを読み取り、その製品が本物であるか、偽物であるかを確認できるシステムを提供すること。
【解決手段】　製品を出荷する際に、そのメーカがその製品を製造したことを証明する証明書データが記録された商品タグ１０１を、商品タグの発行機１０２にて発行して製品に付けて出荷する。店舗において購入者は商品タグ読み取り端末１０３により商品タグ１０１から証明書を読み取り確認する。製品の購入者は、予めネットワーク、郵送などを経由して認証サーバ１０４から証明書解読情報を読み取り端末１０３に入手し、店舗にて商品タグ１０１の証明書情報を照合することにより、その製品が本物であるか、偽物であるかを確認する。



【特許請求の範囲】
【請求項１】　秘密鍵と公開鍵を生成し管理する認証サーバと、該認証サーバで生成した秘密鍵を用いて製品の出所または品質を証明する証明書から電子署名を生成し、該証明書と該電子署名を、電子的なメモリを有する商品タグに書込んで発行する商品タグの発行機と、前記認証サーバで生成した公開鍵を用いて前記商品タグから読み取った証明書の真偽を確認する読取端末を有することを特徴とする製品認証システム。
【請求項２】　請求項１記載の製品認証システムにおいて、
前記読取端末は、前記証明書をハッシュ化して生成した第１のダイジェストメッセージと公開鍵で電子署名を復号化して生成した第２のダイジェストメッセージとを比較して証明書の真贋を判定することを特徴とする製品認証システム。
【請求項３】　製品認証システムに用いる商品タグであって、少なくとも証明書またはハッシュ化された電子署名を含む製品認証のための情報を内蔵メモリに記憶したことを特徴とする非接触式ＩＣカードからなる商品タグ。
【請求項４】　請求項３記載の商品タグであって、
該商品タグを製品に連結するための紐の内部に、当該商品タグを構成する非接触式ＩＣカードの配線の一部を内蔵することを特徴とする商品タグ。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、物品の製品認証（真贋判定）に関し、特に、改竄や製品偽造が防止でき、製造メーカを保護するために有効な製品認証システムおよびそれに用いる商品タグに関する。
【０００２】
【従来の技術】従来、商品の製造元や販売元は消費者に対してその商品の出所や品質を保証するために、商品の製品認証（出所や品質内容の認証）のための証明書を発行していた。その場合の証明書は、紙や布などを用い、署名として印鑑やサインなどが行われるのが普通であった。そのため、簡単に証明書を偽造することが可能であった。この偽造に対する従来の対策としては、透かしやホログラムなどを用いることにより偽造しにくくする方法が講じられていた。
【０００３】また、インターネット上での公開鍵方式による本人認証の技術としては、ＲＳＡ（Rivest Shamir Adleman）暗号化方式を用いる方法などが知られているが、本発明に関連するタグの特許としては、以下のものが挙げられる。特開平９－０５０５０１号公報（タグ）、特開平８－３３５２５７号公報（非接触；ＩＣタグ）、特開平８－１３３４２４号公報（物品の管理方法、管理システム及びそれに適用されるタグ）。
【０００４】
【発明が解決しようとする課題】かかる従来の方法においては、以下のような課題がある。上述したように、ブランド品などの商品に対して製造元（販売元）が出所や内容を証明する証明書は、従来、紙や布などによる表示で行っていて偽造や改竄が容易にできるため、偽造品が市場に氾濫しているのが現状である。このような現状において、製造元（販売元）の利益が侵害され購入者の製品に対する信頼感・安心感が低下し、社会問題化している。また、従来の証明書では偽造や改竄を防止するために透かしやホログラムなどの対策を講じる方法を採用したとしても、それらの対策が講じられていることが購入者に徹底されていなければ、購入者が真贋判定することは困難であるという問題がある。本発明の目的は、上述の問題点を解決し、製品証明書の改竄、製品偽造を防止し、店舗、購入者の製品に対する信頼性の向上を図り、安心感を与えることができるだけでなく、流通段階、税関などにおいても商品の真贋判定ができ、製造メーカの利益を保護することが可能な製品認証システムおよびそれに用いられる商品タグを提供することである。
【０００５】
【課題を解決するための手段】本発明は、上記目的を達成するために、秘密鍵（１０６）と公開鍵（１０８）を生成し管理する認証サーバ（１０４）と、該認証サーバ（１０４）で生成した秘密鍵（１０６）を用いて製品の出所または品質を証明する証明書（１０５）から電子署名（１０７）を生成し、該証明書（１０５）と該電子署名（１０７）を、電子的なメモリを有する商品タグ（１０１）に書込んで発行する商品タグの発行機（１０２）と、前記認証サーバ（１０４）で生成した公開鍵（１０８）を用いて前記商品タグから読み取った証明書の真偽を確認する読取端末（１０３）を有することを特徴としている。さらに具体的には、読取端末（１０３）は、証明書をハッシュ化して生成した第１のダイジェストメッセージと公開鍵で電子署名を復号化して生成した第２のダイジェストメッセージを比較して証明書の真贋を判定することを特徴としている。また、本発明の商品タグは、証明書またはハッシュ化された電子署名を含む製品認証のための情報を内蔵メモリに記憶したものであり、さらに、該商品タグを製品に連結するための紐の内部に、当該商品タグを構成する非接触式ＩＣカードの配線の一部（図２の２０１）を内蔵することを特徴としている。
【０００６】
【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。図１は、本発明の全体システムの概念を示す図である。同図において、１００はネットワーク、１０１は製造メーカが製品につける商品タグ（例えば非接触ＩＣタグ）、１０２は商品タグ発行機、１０３は購入者が店舗で読み取りに用いる読取端末（商品タグリーダ）、１０４は認証サーバ、１０５は出

所や商品品質を証明する証明書、１０６は秘密鍵、１０７は電子署名、１０８は公開鍵である。

【０００７】認証サーバ１０４は、秘密鍵と公開鍵の生成と管理を行っている。商品タグ発行機１０２は、ネットワーク１００を介して認証サーバ１０４から秘密鍵１０６を受け取り、証明書の生成，証明書のハッシュ化による電子署名の生成，商品タグ１０１への証明書および電子署名の書き込み，および商品タグ１０１の発行を行うものである。読取端末１０３は、商品タグリーダ、携帯ＰＣで構成されており、ネットワーク１００を介して認証サーバ１０４から受け取った公開鍵１０８を用いて、読取端末１０３で商品タグ１０１から読み取った証明書および電子署名を照合することにより商品認証を行うものである。

【０００８】図２は、本発明の商品タグ１０１を非接触ＩＣカードを用いて構成した場合の構造例である。本商品タグ１０１は、アンテナ部２０１、メモリ機能を持つＩＣチップ２０２で構成されている。通常の非接触ＩＣタグの配線パターンの一部（電気的に接続されている部分であれば何れの部分であってもよいが、例えばアンテナ部２０１）をタグの紐となる部分の内部に往復するように内蔵させ、製品に取り付ける際に、タグの穴を通して紐の端に樹脂などでストッパー２０３で封止する。本構造を採用すると、封止後に商品タグを商品から外すためには配線パターンの一部（例えば、アンテナ２１０）となっている紐を切らねばならず、商品タグ１０１を商品から外すと同時に商品タグの機能は回路的に破壊されて無効となってしまうため一度商品から外した商品タグは再使用することができず、結果的に商品タグの再使用による悪用を防止することが可能となる。

【０００９】次に、商品タグ発行機１０２の動作を説明する。図３は、商品タグ発行機１０２の動作フローチャートである。同図に示すように、まず、証明書（本文）を生成する（ステップ３０１）。次に、証明書をハッシュ化してダイジェストを作成した後、ネットワーク１００を介して認証サーバ１０４から受け取った秘密鍵１０６で暗号化して電子署名を生成する（ステップ３０２）。次に、商品タグ１０１と通信を開始し（ステップ３０３）、前記生成した証明書（本文）と電子署名を商品タグのメモリ内へ書き込む（ステップ３０４）。

【００１０】次に、読取端末１０３の動作を説明する。図４は、読取端末１０３の動作フローチャートである。同図は既にネットワーク１００を介して認証サーバ１０４の公開鍵１０８を入手した後の動作を示している。まず、読取端末１０３は、商品タグ１０１との通信を開始し（ステップ４０１）、商品タグ１０１のメモリ内に格納されている証明書と電子署名を読取端末１０３へ読み込む（ステップ４０２）。次に、証明書（本文）をハッシュ化して第１のダイジェストメッセージＡを作成する（ステップ４０３）。さらに、電子署名を公開鍵を用いて復号化し第２のダイジェストメッセージ（ダイジェストメッセージＢ）を作成する（ステップ４０４）。この第１のダイジェストメッセージＡと第２のダイジェストメッセージＢを比較して一致するか判断する（ステップ４０５）。一致すれば本物であることを読取端末１０３の表示部に表示し（ステップ４０６）、もし一致しなければ、偽造品であることを同じく読取端末１０３の表示部に表示する（ステップ４０７）。

【００１１】図５は、秘密鍵／公開鍵を用いた認証アルゴリズムを説明するための模式図である。以下、図３と図４の各ステップと対応付けて該認証アルゴリズムを説明する。商品タグ発行機１０２は、まず、（イ）証明書を生成し（図３のステップ３０１）、（ロ）証明書をハッシュすることによりダイジェストを作成し、（ハ）該ダイジェストメッセージを秘密鍵１０６で暗号化して電子署名を生成する（同ステップ３０２）。（ニ）証明書と電子署名を商品タグ１０１のメモリ内に書き込む（同ステップ３０３，３０４）。（ホ）商品タグ１０１から証明書と電子署名を読み出し（図４のステップ４０１～４０２）、証明書をハッシュして第１のダイジェストメッセージＡを作成するとともに（同ステップ４０３）、（ヘ）電子署名を公開鍵１０８で復号化し第２のダイジェストメッセージＢを作成し（同ステップ４０４）、（ト）該作成した第１のダイジェストメッセージＡと第２のダイジェストメッセージＢを比較し、その一致／不一致によって本物／偽物を判別する（同ステップ４０５～４０７）。

【００１２】上述した実施例では、秘密鍵１０６と公開鍵１０８の受け渡しをネットワーク１００を介して実施する例を説明したが、これに限定せず、紙，フロッピーディスク（ＦＤ），メモリカード，ＩＣカード，ＣＤ－ＲＯＭ，光磁気ディスク，ＤＶＤなどの記録媒体を用いて直接の手渡しや、郵送によるオフラインの受け渡しであってもよい。さらに、上述した実施例では、商品タグ１０１に記録する内容として証明書と電子署名の例を説明したが、その他の例として、❶ 証明書のみ、❷ 証明書＋暗号化された証明書、❸ 暗号化された証明書のみであってもよい。さらに、上述した実施例では、本発明の活用場所として、購入者が店舗にて活用する例を説明したが、製造メーカから卸店へ卸す過程や卸店から小売り店舗などに卸す過程などの各種流通過程、または税関などにおいても本発明が活用できることはいうまでもない。

【００１３】

【発明の効果】以上説明したように、本発明によれば、製品認証商品タグによって、製品証明書の改竄、製品偽造を防止し、製造メーカの利益を保護できる。また、読取端末により容易に商品の真贋判定が容易に行える。これにより店舗、購入者の製品に対する信頼性の向上を図り、安心感を与えることができるだけでなく、流通段階、税関などにおいても商品の真贋判定ができるなどの

優れた効果が奏される。

【図面の簡単な説明】

【図１】全体システムを示す図である。

【図２】商品タグの構造を示す図である。

【図３】商品タグ発行機の動作を示すフローチャートである。

【図４】読取端末の動作を示すフローチャートである。

【図５】秘密鍵／公開鍵を用いた認証アルゴリズムを説明するための模式図である。

【符号の説明】

１０１：商品タグ

１０２：商品タグ発行機

１０３：読取端末

１０４：認証サーバ

１０５：証明書（本文）

１０６：秘密鍵

１０７：電子署名

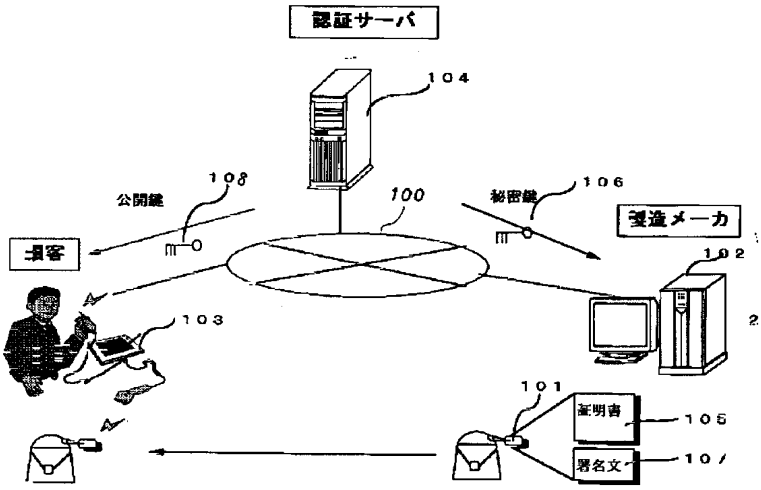
１０８：公開鍵

２０１：商品タグの配線パターンの一部（例：アンテナ）

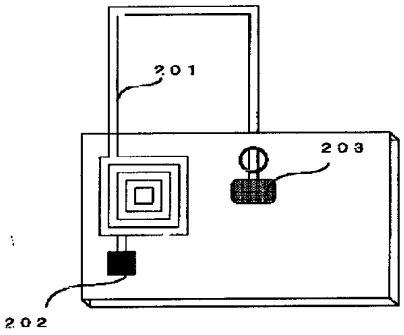
２０２：非接触ＩＣタグ内部のＩＣチップ

２０３：商品タグのストッパー（封止）

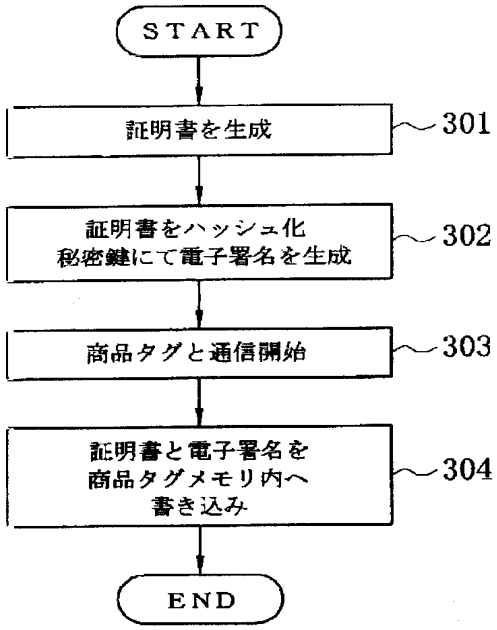
【図1】



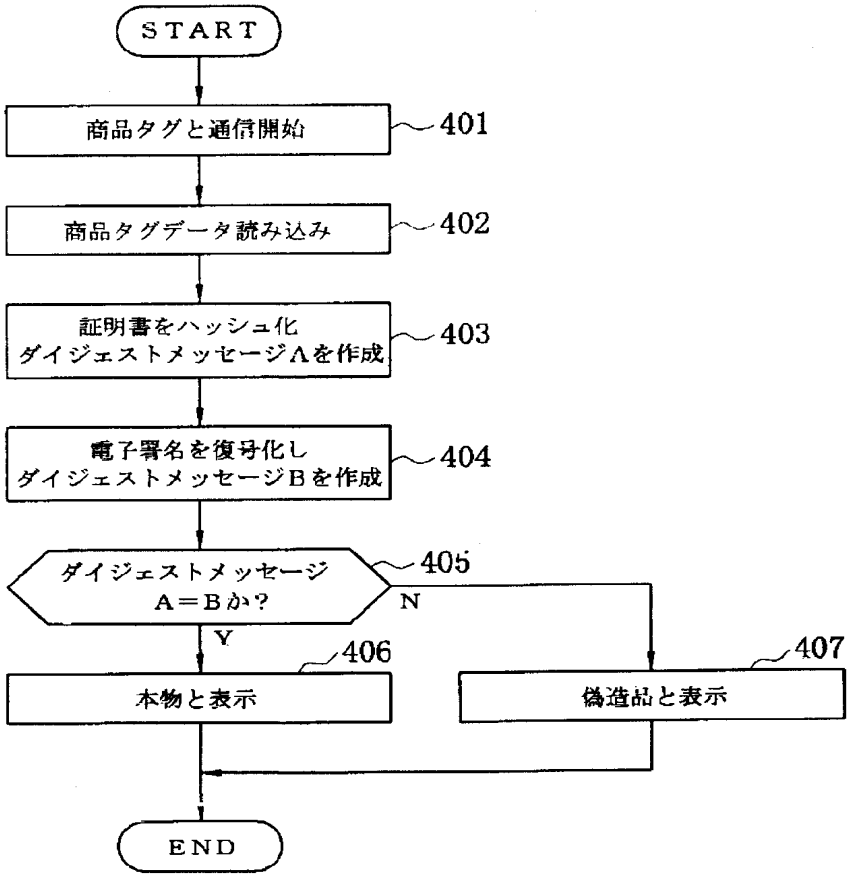
【図2】



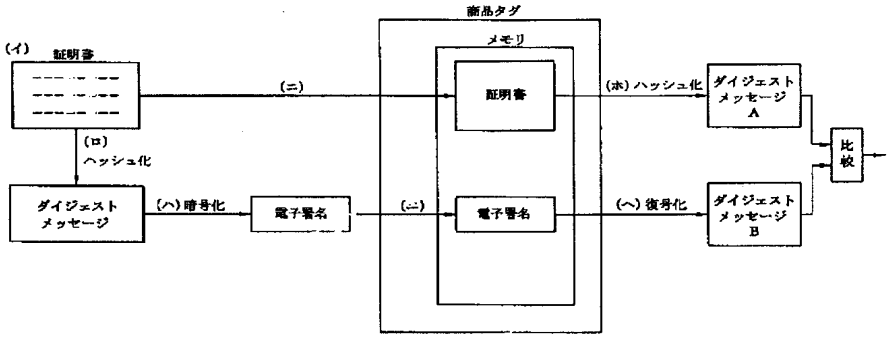
【図3】



【図4】


START
商品タグと通信開始
401
商品タグデータ読み込み
402
証明書をハッシュ化
ダイジェストメッセージAを作成
403
電子署名を復号化し
ダイジェストメッセージBを作成
404
ダイジェストメッセージ
A＝Bか？
405
N
Y
406
本物と表示
407
偽造品と表示
END

【図5】


商品タグ
メモリ
(イ) 証明書
(ロ) ハッシュ化
ダイジェストメッセージ
(ハ) 暗号化
電子署名
(ニ)
証明書
(ホ) ハッシュ化
ダイジェストメッセージA
(ヘ) 復号化
ダイジェストメッセージB
比較

フロントページの続き

Ｆターム(参考)　5B035 AA14 CA23 CA38
5B049 BB11 CC23 CC28 DD04 EE03
EE09 EE23 FF03 FF04 FF08
GG04 GG07 GG10
5B058 CA27 KA06 KA32 KA35
5K013 BA02 FA03 GA00 GA08